

REMARKS

This Request for Reconsideration is responsive to the Final Office Action dated February 7, 2006. Claims 1-36 remain pending in the application. Claims 1, 14, 23, and 36 are independent claims. Reconsideration of the pending claims is requested in consideration of the claim amendments and the following remarks.

Applicant acknowledges and appreciates the withdrawal of the rejection of the claims under 35 U.S.C. § 112.

Claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32 and 34-36 remain rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 6,035,402 to Vaeth et al. ("Vaeth"). This rejection is traversed.

Independent claim 1 recites: *[a] public key certificate issuing system comprising:*

*a certificate authority for issuing a public key certificate used by an entity; and
a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;*

wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

Applicant again submits that these claimed features are neither disclosed nor suggested by Vaeth.

Vaeth discloses a Virtual Certificate Authority (VCA) wherein requests for a certificate and verification information are directed to the Certificate Authority (CA) from a Request Authority (RA). The CA may include a plurality of crypto-cards each implementing different cryptography functions. Each crypto card is associated with a single cryptography function. The RA is the entity with verification responsibilities. The RA receives certificate requests from a plurality of requesting entities, for example, a merchant, a payment gateway, and a cardholder. The CA implements generic or specialized certificate functions based on the requesting entity (col. 7, ll. 36-40), which make use of the cryptography algorithms stored on the crypto cards. The CA creates each type certificate by using a different cypto-card to perform to associating cryptography functions, thereby creating a one-to-one **relationship between certificates types and entity types**. This allows a single RA 180 to issue each given type of requesting entity an associated type of certificate. Furthermore, Vaeth teaches that since the certificates are associated to the type of entities, it is possible to have different RAs (180 and 188) issue similar certificates or work jointly to issue certificates via the same CA using joint approval schemes (col. 7, ll. 49-59).

Applicant submits that Vaeth does not teach or suggest that the Control Authority “*selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm.*” Instead, Vaeth teaches selecting which algorithms to perform and certifications to issue based on the entity that is requesting the certificate, by associating specific cryptographic function (or groups of functions) with merchant requests, another with cardholder requests, and yet another with payment gateway requests. Vaeth does not identify the assigned algorithm based on the Registration Authority, because doing so would run contrary to Vaeth’s purpose of being able to provide different certificates through the same Registration Authority. Similarly, doing so would also make it impossible for Vaeth to perform joint approval schemes using multiple Registration Authorities.

The Examiner cited Vaeth col. 8, ll. 35-48, for the allegation that Vaeth does in fact teach

that “*said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm.*” Applicant submits that these lines only indicate that the RA acts as a gatekeeper between the transacting entity and the CA. The cited paragraphs do not teach or suggest that the CA considers which RA forwards a given request when associating the given requests with a function and certification. While such information may be pertinent for network transmission purposes, there is no indication whatsoever that this information plays any role within Vaeth’s crypto-card/certification selection scheme. The examiner’s allegation also fails to take into account Vaeth’s disclosure of performing joint certification, which would further dissociate any certification selection from a given RA, since under such a scheme multiple RAs provide requests for the same types of certificates.

Vaeth therefore fails to disclose, teach, or suggest various features of independent claim 1. For similar reasons, independent claims 14, 23, and 36 are also neither disclosed nor suggested by Vaeth (although claims 1, 14, 23, and 36 should be interpreted solely based upon the limitations set forth therein).

Accordingly, Applicant respectfully requests that the rejection of independent claims 1, 14, 23, and 36 and dependent claims 2, 3, 5, 6, 9, 10, 12, 13, 15-17, 19, 20, 22, 24, 25, 27, 28, 31, 32, 34 and 35 under 35 U.S.C. § 102(b) be withdrawn.

Claims 4, 7, 26, and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of U.S. Pat. No. 6,202,157 to Brownlie et al. (“Brownlie”); Claims 8, 18, and 30 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of Boneh et al., “On the Importance of Checking Cryptographic Protocols for Faults” (“Boneh”). Claims 11, 21, and 33 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of U.S. Patent No. 6,675,296 to Boeyen et al. (“Boeyen”). These rejections are traversed.

As previously described, Vaeth does not disclose, teach, or suggest at least the features of selecting “*at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an*

assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm” as recited in independent claim 1, and similarly stated in independent claims 14 and 23. Dependent claims 4, 7, 8, and 11 depend on independent claim 1, and therefore include the features of independent claim 1. Dependent claims 18 and 21 depend on independent claim 14, and therefore include the features of independent claim 14. Dependent claims 26, 29, and 33 depend on independent claim 23, and therefore include the features of independent claim 23.

Brownlie discloses a network security system capable of applying security policy provisions issued at a centralized authority to various network nodes, which in turn verify the policy provisions using digital signatures associated with the central authority. Boneh describes how various authentication protocols can be broken using hardware faults. Boeyen discloses a certificate issuing apparatus and method to facilitate converting certificates between different formats. The Boeyen apparatus employs a series of templates representing different certificate formats, and maps the relevant data between the different formats. Neither Brownlie, Boneh, nor Boeyen disclose or suggest selecting an encryption algorithm with reference to a table that associates the registration authority with an assigned signature algorithm, all features that are also absent from Vaeth as described above.

Even assuming, *arguendo*, that Brownlie, Boneh, Boeyen, and Vaeth were combinable, Applicant submits that none of the cited references, either alone or in any proper combination, cure the deficiencies of Vaeth with respect to at least the previously identified features of claim 1, 14, and 23.

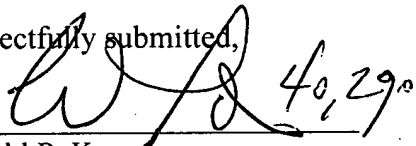
Therefore, Applicant respectfully requests that the rejection of claims 4, 7, 8, 11, 18, 21, 26, 29, and 33 under 35 U.S.C. § 103(a) be withdrawn.

CONCLUSION

In view of the above Request for Reconsideration, applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-2320 from which the undersigned is authorized to draw.

Dated: March 30, 2007

Respectfully submitted,
By 
Ronald P. Kananen
Registration No.: 24,104

Christopher M. Tobin
Registration No.: 40,290

RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
Attorneys for Applicant

Attachments: Amendment Transmittal

DC270979.DOC